



Do not find bugs;  
Bugs find you



# Daunting Bug Hunting?



Bug hunting:

- Is fun and cool
- Can be daunting...

Can we avoid that feeling?



# Vulnerability Research

- Do I find a bug?
- Is it exploitable and severe?
- Does a vendor accept?
- How long does it take?

You can fail, feel exhausted

# Security Study

- Focus on learning
- OK with not finding bugs

Cannot fail

Investment for further analysis,  
deep bugs

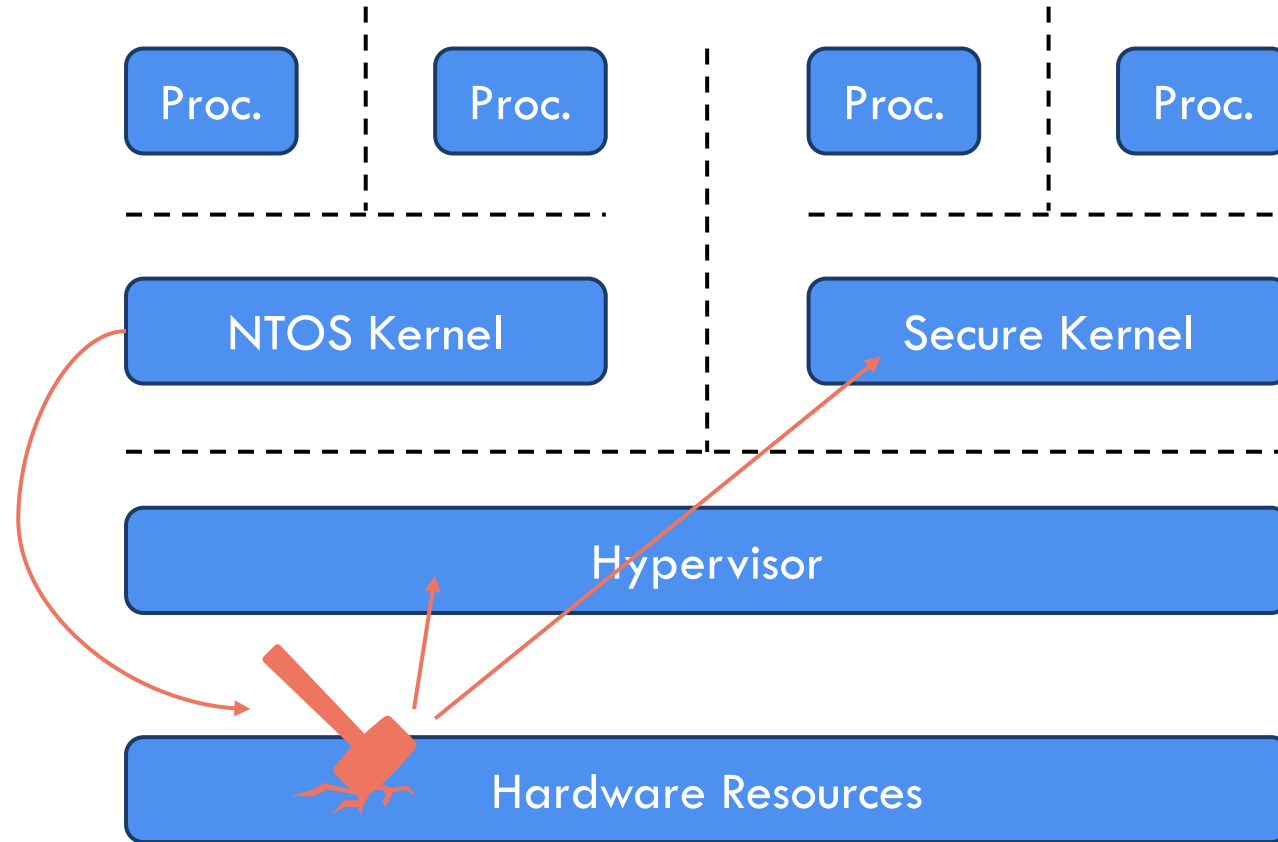




# Cases

1. Windows Hypervisor bugs
2. VT-rp study

# Modern windows security model



# Windows Hypervisor Bugs

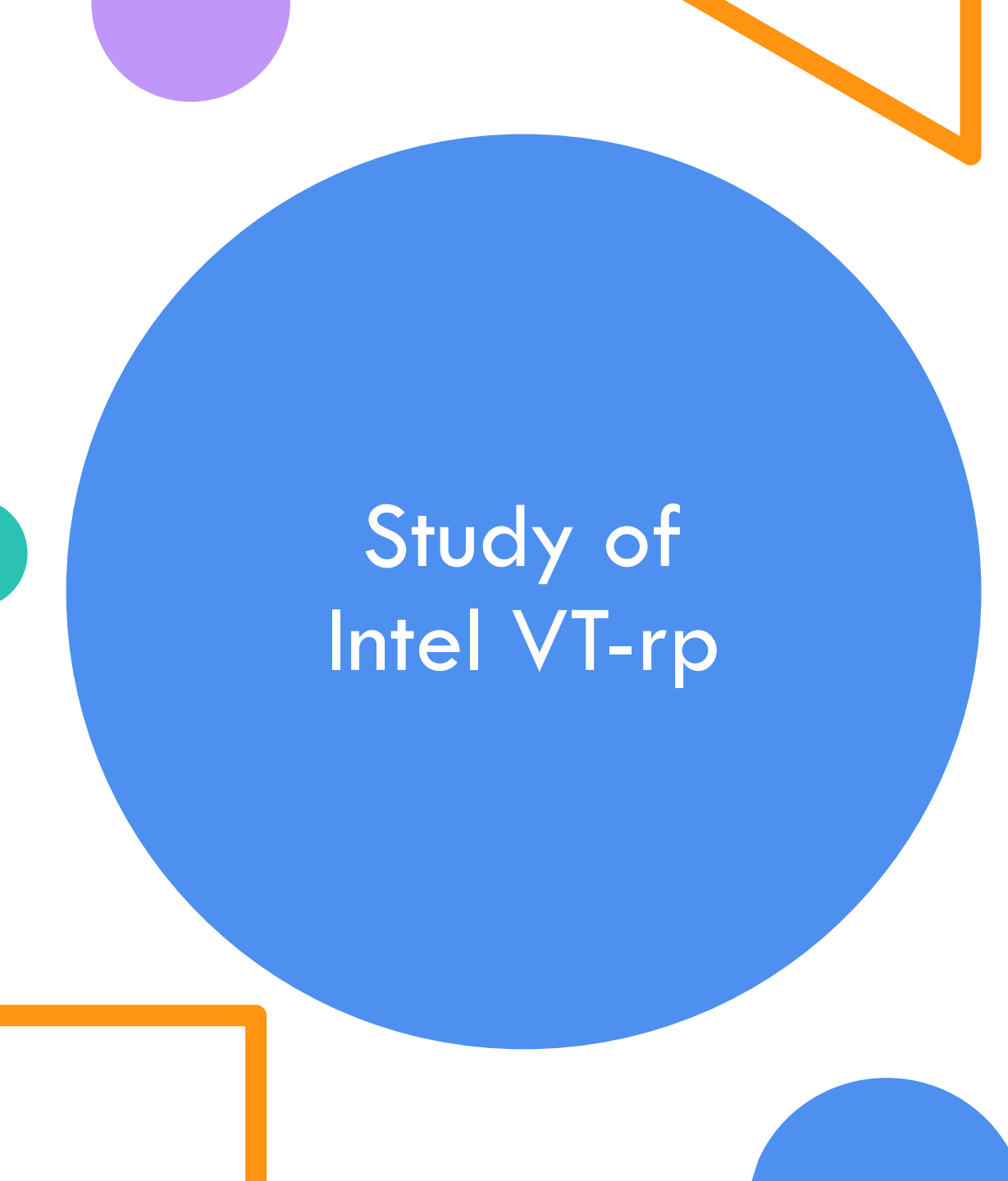
[CVE-2023-36427](#) & [CVE-2024-21305](#)

By-products of studying Windows' virtualization-based security

Interesting bugs

- ✓ Blog
- ✓ Talk
- ✓ Extra money 💰

Research idea: AMD counterpart



# Study of Intel VT-rp

Security feature on Intel 12+ gen

No bug, but ended up with an  
exciting opportunity

- ✓ Blog
- ✓ Talk
- ✓ Free trip to Montreal ✈️

Security study itself can be fun and  
rewarding



# Security Study

Can naturally

- Let you build skills and experience
- Yield output
- Avoid emotional rollercoasters

[Watch keynote by Mark Dowd @ OffensiveCon](#)

- Works for both casual and experienced, full-time hunters





# Conclusion

1. Focus on learning
2. View your learning as progress and success
3. Do not find bugs



# About myself

- Satoshi Tanda

 [in/satoshitanda](https://www.linkedin.com/in/satoshitanda)

 [@satoshi\\_tanda@infosec.exchange](mailto:@satoshi_tanda@infosec.exchange)

 [@standa\\_t](https://twitter.com/standa_t)

 [@tandasat](https://github.com/tandasat)

- System software engineer, researcher and trainer with 15+ years of experience
- Vancouver local since 2012
- Got first job here via VanCitySec ❤️